The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:

07/31/2014

SUBJECT:

Multiple Vulnerabilities in Cisco IronPort Encryption Appliance Could Allow Remote Access or Unauthenticated File Access

OVERVIEW:

Multiple vulnerabilities have been discovered in Cisco IronPort Encryption Appliance. Cisco IronPort Encryption Appliance devices contain two vulnerabilities that allow remote, unauthenticated access to any file on the device and one vulnerability that allows remote, unauthenticated users to execute arbitrary code with elevated privileges.

SYSTEMS AFFECTED:

Cisco IronPort Encryption Appliance 6.5 versions prior to 6.5.2
Cisco IronPort Encryption Appliance 6.2 versions prior to 6.2.9.1
Cisco IronPort PostX MAP version prior to 6.2.9.1

RISK:

Government:

Large and medium government entities: **High**
Small government entities: **High**

Businesses:

Large and medium business entities: **High**
Small business entities: **High**

Home users: N/A

DESCRIPTION:

The Cisco IronPort Encryption Appliance contains two information disclosure vulnerabilities that allow remote, unauthenticated access to arbitrary files on vulnerable devices via the embedded HTTPS server. The first vulnerability affecting the Cisco IronPort Encryption Appliance administration interface is documented in IronPort bug 65921 and has been assigned Common Vulnerabilities and Exposures (CVE) identifier CVE-2010-0143. The second vulnerability affecting the WebSafe servlet is documented in IronPort bug 65922 and has been assigned Common Vulnerabilities and Exposures (CVE) identifier CVE-2010-0144.

The Cisco IronPort Encryption Appliance contains a remote code execution vulnerability that allows an unauthenticated attacker to run arbitrary code with elevated privileges on vulnerable devices via the embedded HTTPS server. The vulnerability is documented in IronPort bug 65923 and has been assigned Common Vulnerabilities and Exposures (CVE) identifier CVE-2010-0145.

RECOMMENDATIONS:

The following actions should be taken:

Upgrade to a fixed version or follow the workarounds described for all vulnerable Cisco products immediately after appropriate testing.

REFERENCES:

CISCO:

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20100210-ironport

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0144

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0145